Fermilab Policy on Computing

Abstract

This is an abstract of the Fermilab Policy on Computing. The full text of the Policy follows the abstract at http://www.fnal.gov/cd/main/cpolicy.html. *For details and who to go to when authorization for an activity is required, please consult the full text of the Policy. If you find something unclear or ambiguous in this abstract, see the full Policy for the final word. Feel free to address questions to Irwin Gaines (x4022, gaines@fnal.gov) or to another computer security person listed in the Policy's section on "Roles".*

Fermilab's Policy on Computing covers all Fermilab-owned systems and all systems, regardless of ownership, when connected to our network (or showing a Fermilab address). You are responsible for the actions of any person whom you permit to use Fermilab computing or network resources through an account assigned to you.

Appropriate Use

Fermilab encourages effective use of computing technologies in all aspects of its activities. Fermilab maintains an open scientific environment where the free exchange of ideas is encouraged and protected. We permit a wide range of computer activities including incidental use for private purposes. We encourage use of the Web and other Internet communication channels. With this comes the responsibility for every Fermilab employee and user to exercise common sense and good judgment.

Our policy is consistent with Federal (GSA) guidelines. However, many members of the public do not understand the scientific culture of openness and may question a posting (or email) that shows an FNAL.GOV address if it is not clearly related to Fermilab's scientific mission. Therefore, from a Fermilab address you should avoid highly visible activities on newsgroups, auctions, game sites, etc., that are not clearly Fermilab business. In particular, avoid all such Internet activities that are in competitive and/or contentious environments (auctions, political news groups, etc.) and avoid acting as a public server of music or other media unrelated to our mission. It is Fermilab policy to respect the intellectual property rights of others including copyrights, trademarks, and software licenses.

Use common sense in displaying links on pages with Fermilab addresses. Web crawlers (Yahoo, etc.) index all pages they can see. Even accidentally inappropriate wording may be indexed. You can direct web crawlers to ignore pages that you do not need to be found through search engines. See http://www.fnal.gov/cd/webgroup/webhelp/access.html. Semi-official pages and pages intended for the public are required by the DOE to carry a notice. Include a link on each such page to http://www.fnal.gov/pub/disclaim.html

The following are explicitly NOT permitted:

- Legally prohibited activities;
- Activities that reasonably offend other employees, users, or outsiders, or results in public embarrassment to the laboratory;
- Activities in support of an ongoing private business;

- Up- or down- loading or viewing of sexually explicit material.

You must have specific approval for activities that consume significant amounts of computer or network resources whether for lab or personal purposes.

Rules to Protect Fermilab Computing

Our first lines of defense are the individuals responsible for data and the local system managers. Proper use and protection of passwords, physical protection of computers, and regular backup of important data are required. The Fermilab Policy on Computing includes a minimal set of strongly enforced specific rules. In addition, any form of blatant disregard for computer security is not tolerated.

- You are required to immediately report any suspected computer security incidents to 630-840-2345. The Fermilab Computer Incident Response Team (FCIRT) investigates incidents. The Head of FCIRT may assume full administrative control of affected systems until the incident is resolved, call on other experts for priority assistance and direct local system managers to respond to the situation. You may not disclose information regarding a computer security incident without authorization.
- Hacking is forbidden, including unauthorized attempts to gain access, to damage, alter, falsify, or delete data, to falsify email or network address information, or to cause a denial of computing or network service. The use or possession of security-probing or cracker tools requires written authorization.
- You may not implement network or email infrastructure services without written authorization.
- If you have privileged access to three or more systems, to a major clustered system, or to any computer within a critical system domain, you are required to register through the web form at http://miscomp.fnal.gov/sysadmindb and to follow security guidelines.
- No one may inspect another person's files or email without that person's permission or other authorization, explicit or implicit, as described in the Policy.
- You must not allow anyone else to know or use your Kerberos password. Don't use your Kerberos password for other than Fermilab Kerberos. Do not transmit Kerberos passwords (or the character string of a Kerberos password) across the network. In the rare circumstances where transmitting a Kerberos password is necessary, it must be strongly encrypted. Never store Kerberos passwords (or the corresponding character strings) on a computer, encrypted or not. Configuration rules (see Sec. IV) for Kerberos-protected systems must not be circumvented.

Use of Computers in Systems that Protect People, Property, or the Environment

Fermilab policy is to avoid reliance on a computer as an essential element of any system that is necessary to protect people from serious harm, to protect the environment from significant impact, or to protect property the loss of which would have a serious impact on our mission. The use of computers for monitoring, data logging, and reporting is encouraged, however computers used for these purposes must not be essential for protection. Contact the Fermilab Computer Security Executive for any variance.

Fermilab Policy on Computing

Advances in the basic understanding of elementary particles have through a long history been enabled by the ever-changing frontiers of technology. Computing has always been one of the key technologies that enable the science, and this is particularly true today. Fermilab encourages effective progressive use of computing technologies in all aspects of its activities, recognizing that this brings with it special, always evolving, concerns.

Computing is one of many tools used at Fermilab and, as such, general policies, written and unwritten, that govern life at Fermilab apply equally to computing. For example, it is obvious that the same rules of ethical behavior apply regarding fraud, forgery, plagiarism, harassment, libel, etc. whether computers are involved or not. However, the ability of modern computers and networks to manipulate, store, and broadcast information is so extraordinarily powerful that it changes many qualitative aspects of how we function in a research laboratory, often in dramatic ways.

The policies and rules described in the following are intended to address these special aspects of computing at Fermilab. The policy is divided into four sections:

1. Policies and Rules to Protect Fermilab Computing
2. Publishing and Accessing Information on Electronic Networks
3. Use of Computers in Systems that Protect People, Property, or the Environment
4. Special Policies and Rules for the Strong Authentication Realm

1. Policies and Rules to Protect Fermilab Computing

The communications needs for research and planning require a broad openness in our systems. Our main concerns are protecting data and systems critical to the operations of the laboratory in pursuit of its mission. Fermilab's continuing policy has been to put its first line of defense at the individual responsible for the data and the local system manager. Proper use of passwords and, most importantly, backup of important data is what we expect of our computer users and system managers.

Roles

The Director has delegated overall responsibility for computer security and related matters to the Fermilab Senior Computer Security Executive (CSExec).The Fermilab Computer Security Coordinator (FCSC)[1] FCSC reports to the CSExec in this area, and is the laboratory's principal

[1] The CSExec responsibility is currently assigned to the Director's Special Advisor on Computing and Government Policy, Thomas Nash, 630 840 3203, nash@fnal.gov. Matthias Kasemann, 630 840 6387, kasemann@fnal.gov, is Deputy CSExec, and Dane Skow, 630 840 4730, dane@fnal.gov, is Alternate CSExec. The FCSC role has much in common with what was previously called the Computer Protection Program Manager (CPPM). The FCSC is Matt Crawford, 630 840 3461, crawdad@fnal.gov. The General Security Domain Coordinator is Irwin Gaines, 630 840 4022, gaines@fnal.gov. Donna Dyxin is the Deputy FCSC for Government Liaison, 630 840 8849, ddyxin@fnal.gov.

day to day computer security manager and lead point of contact with external organizations (DOE, FBI, CIAC, etc.) on computer security. In the latter role, the Deputy FCSC for Government Liaison assists the FCSC, particularly in handling policy communications with the DOE. A second Deputy FCSC is the General Security Domain Coordinator.

Scope

Fermilab's Computer Security Policy covers Fermilab systems[2], whether on-site and connected directly to the Fermilab network, or on- or off-site and connected to the Fermilab network by the telephone system, the Internet, or other means. The policy and rules described here cover these systems no matter who is the owner or the method of connection to the network.

Not included are those activities by users of off-site computers that do not involve, and do not give the appearance of involving[3], computers on the Fermilab site network.

Additional security rules apply to the configuration of all on-site or off-site computers within Fermilab's "Strengthened Realm".[4] (See Section 4).

Fermilab employees and registered users are responsible for their own actions under the computer security policy, as well as for the actions of any person who they permit to access a Fermilab system.[5]

Appropriate Use

Fermilab's single mission is science and the laboratory's stated policy is to maintain an open scientific environment where the free exchange of ideas is encouraged and protected. We want there to be unhindered freedom to use computers within a wide area, but this area is surrounded by extremely high walls. We cannot always describe exactly where those boundaries lie, because the technology is changing rapidly and because the walls may shift with shifts in the public's tolerance and areas of scrutiny. Those who use Fermilab's computers and networks will have to use judgment and common sense when they operate near the edges of acceptable use. Examples of activity that may bring an employee or user near or past walls of acceptable usage and incur serious disciplinary repercussions (or, in certain cases, criminal sanctions) are:

---

[2] "Fermilab systems" are those which are connected to the network and show an address or name within a Fermilab network or domain (e.g. 131.225.*.*,fnal.gov, sdss.org, auger.org, etc.), as well as systems not connected to the network but owned by Fermilab.

[3] Show an address, name, or email address within a Fermilab network or domain (e.g. 131.225.*.*,fnal.gov, sdss.org, auger.org, etc.).

[4] On-site or off-site computers in the "Strengthened Realm" are those on which users may be authenticated for access to systems on the Fermilab network by a Fermilab Kerberos Key Server.

[5] Some operating system user identifiers (such as root or Administrator) are understood to be commonly shared by several people. Other user identifiers are explicitly shared for various roles or projects. A user's Kerberos identifier is never to be shared. The proper way to share access to a Kerberos-protected resource or service is to list the user principals in an ACL file such as .k5login.

- Legally prohibited activities on the Internet (child pornography, interstate gambling,…);
- Computer usage that reasonably offends other employees, users, or outsiders, or results in public embarrassment to the laboratory;
- Computer usage that is not specifically approved and which consumes significant amounts of computer resources not commensurate with its benefit to the laboratory's mission or which interferes with the performance of an employee's assigned job responsibilities;
- Operation of a private business or social activity unrelated to the laboratory;
- Violation of license and other computer related contract provisions, particularly those that expose the laboratory to significant legal costs or damages.

Questions of proper or improper use of computers are normally management rather than technical issues and should be dealt with in the normal course of supervisory oversight. The Computer Security Plan includes the necessity of rapid response investigation of incidents involving extreme behavior, as well as preventive monitoring where there is reasonable cause.

Rules

The Computer Security Plan provides a minimal set of rules that will be enforced. They address incident reporting, protection of system and network integrity, prohibitions against unauthorized activities, ethical behavior, etc. They address matters serious enough that the laboratory is willing to enforce disciplinary measures for first offenses, such as suspending employees or barring users from laboratory facilities.

Incident Reporting

All employees and users are required to immediately report any suspicious incidents involving the security of Fermilab computers or networks, including apparent attempts at unauthorized access. Incidents should be reported to the Feynman Computing Center 24x7 Customer Support Help Desk at +1 630-840-2345, or to the system manager if immediately available. System managers are expected to report incidents immediately that do not have a simple explanation based on normal routine operation of the system. If there is clearly no urgency, incidents may be reported by email to computer_security@fnal.gov.

Incidents which must be reported include computer- or network-related activity, internal or external to Fermilab, that may impact Fermilab's mission through, for example, the possibility of: loss of data; denial of services; compromise of computer security; unauthorized access to data that Fermilab is required to control by law, regulation, or DOE orders; investigative activity by legal, law enforcement, bureaucratic, or political authorities, or a public relations embarrassment.

The Fermilab Computer Incident Response Team (FCIRT), appointed by the CSExec, will investigate all reported incidents. Incidents are quickly triaged by FCIRT. During particularly serious incidents known as "FIREs[6]", the Head of FCIRT may assume full administrative control of affected systems until the incident is resolved, and may call on other technical experts for priority assistance. For incidents with localized implications,

[6] "Fermilab Incident Response Emergency"

the Head of FCIRT may declare a "SMOKE[7]" and direct local system managers to respond to the situation under the oversight of FCIRT.

Employees and users must not disclose information resulting from a computer security incident without authorization. The head of the FCIRT and the CSExec, in consultation with the head of the Computing Division and the Public Information Office, will determine specific information to be disclosed to employees, users, other organizations, and the public.

Unauthorized and Malicious Access and Actions

All employees and users are forbidden to attempt unauthorized entry to computer systems or accounts, or to attempt unauthorized damage, alteration, falsification or deletion of data (including software and email). This prohibition explicitly includes attempts to spoof or falsify email, network, or other information used to identify sources, destinations or other information about communications, data, or storage. Individuals are implicitly authorized to access accounts in their own name, and to alter or delete data in those accounts, and they may access files which are enabled for reading for a class of individuals including the person attempting to access them. The burden of proof of authorization rests with the person attempting to access an account; possession of a password is not proof of authorization. All employees and users are forbidden to attempt to cause denial of computing or network services at Fermilab. Serious negligence that results in service denials will be treated as any other negligence that results in equivalent damage to the laboratory mission.

Blatant Disregard for Laboratory Computer Security

Blatant disregard for Laboratory computer security will not be tolerated. The FCSC or Head of FCIRT (or their designees) may advise individual employees or users that specific computer security practices are unacceptable in a way which unreasonably exposes Fermilab computers or increases the effort required by computer security personnel, and that they should correct these unreasonable practices. Email records of such "warnings" or "advisories" will be maintained by the FCSC's organization. If an employee who has received such a written "warning" or "advisory" about an unacceptable practice is found, either through routine security evaluations or through an FCIRT investigation of an incident, to be again in violation in regard to this practice, the FCSC will refer the case to the CSExec for disciplinary action.

Individuals who, by reason of their actions or the configuration or content of computer systems for which they are responsible, have been implicated as a significant factor causing a serious computer security incident (FCIRT triaged as a SMOKE or FIRE) should become especially aware of computer security rules and guidance. Being implicated as a significant factor in a subsequent serious computer security incident will be taken as *prima facie* evidence of blatant disregard for computer security.

[7] "System Manager's OKurrence Evaluation"

Restricted Central Services

The following services may only be implemented by Computing Division personnel authorized in writing by the Computing Division Data Communications Group Leader, or as otherwise noted:

- Routing and bridging, except that the Beams Division runs its own subnets.
- Tunneling, except tunnels with a single source or destination for purposes of mobility or security.
- All forms of off-site network connection except modems.
- DHCP.
- Assignment of IP and DECNET host names and addresses. (Use of automatic configuration mechanisms provided by the Computing Division Data Communications Group, such as DHCP, are not restricted.)
- DNS zone mastering and all externally-reachable DNS service.
- NTP time service at stratum 1. (Stratum 2 server operation is discouraged.)
- NNTP.

Specific waivers from these restrictions must be in writing and may be granted only by the FCSC or the Computing Division Data Communications Group Leader. Waivers granted to non Fermilab employees require the concurrence of the CSExec.

The following services are also restricted. Exceptional approval for professionally managed workgroup-local implementation will be considered by the FCSC.

- Externally-reachable email servers, including SMTP, POP and IMAP.
- Kerberos key servers.

Security and Cracker (or Hacker) Tools

A "security tool" is a tool with the capability to systematically probe, or otherwise gather information about, a system or network in order to discover security vulnerabilities. A "cracker tool" (often referred to as a "hacker tool") is a tool with the capability to systematically exploit security vulnerabilities in order to attempt unauthorized access, destruction or theft of data, denial of service, or other unauthorized activities. The use of any tool as a security or cracker tools, or the possession of any tool whose principal capability is as a security or cracker tool or to disguise or facilitate cracking or security probing activities, by employees and users is limited to the specific tools, time frame, and purpose, in explicit written authorization signed by the CSExec or FCSC.

System Managers

Employees and users who have root/system/administrator password access to three or more systems, or to a major clustered system, or to a computer within a critical system domain, are required to register with the FCSC (via the web form at http://miscomp.fnal.gov/sysadmindb) so they may be reached to provide assistance during a computer security incident response. They will be asked to maintain a list of all systems

for which they have root access. All system managers will be expected to follow sound system security guidelines as developed by the Computing Division.

System managers may access all "system" accounts and files on systems for which they have responsibility. "System" accounts and files are those not specifically assigned to an individual. In the course of normal system maintenance activities they may disable the computer or its network connections and they may work with an individual's account or files with the following restrictions: they may not physically (in the human sense) read or inspect the data or information in them (except for files enabled for reading by a class of individuals including the person attempting to read them), and they may not change or delete files in a way that precludes recovering the original data. A person has "system manager responsibility", if a) he/she is registered in the System Manager Data Base for that system; or b) the system is assigned as an individual computer or workstation to the person (and registered in the sensitive item database if applicable).

Data Integrity and Backup

Users ("data owners") are responsible for determining what data requires protection and how their data is to be recovered if the online copy is destroyed (either by accidental or malicious damage). They may choose not to back up data, but if so they must make sure they know how to recreate the lost data if needed. If backup is necessary then the users must coordinate a backup plan. This may either be an individual backup done by the users themselves or coordinated with the system managers into a regular system backup plan.

System managers are responsible for carrying out the backup plans for the systems they manage. They are expected to publish to their users the following: a) which files and data on the system are backed up and which are not; b) backup procedures including frequency of backup, type of backup (full or incremental), media, procedure for restoring files, and location of media storage; c) any special local storage management policies (e.g. automatic purging of backed up areas). System managers are also responsible for periodically testing restoration procedures and for recording the dates of backups, success or failure, and results of restoration tests.

Protection of Kerberos Passwords

You must not allow anyone else to know or use your Kerberos password. Don't use your Kerberos password for other than Fermilab Kerberos. Do not transmit Kerberos passwords (or the character string of a Kerberos password) across the network. In the rare circumstances where transmitting a Kerberos password is necessary, it must be strongly encrypted. Never store Kerberos passwords (or the corresponding character strings) on a computer, encrypted or not. Configuration rules (see Sec. IV) for Kerberos-protected systems must not be circumvented.

Division/Section/Large Experiment Rules

Divisions and sections and large experiments[8] may establish security rules or guidelines for systems under their management. These may be enforced by disabling access for a user who is in violation.

Critical Systems

Computer security incidents involving certain systems could seriously impact the laboratory's science programmatic operations. Such systems may be designated "critical systems" and may be subject to additional computer security policies and procedures, beyond those described here.

Privacy of Electronic Files and EMail

In normal day to day activities, Fermilab respects the privacy of the electronic files and email of employees and visitors, and it expects all employees and visitors to do likewise. No one may inspect the files or email belonging to anyone else on a Fermilab computer without that person's permission, either explicit or implicit as described above in the rule "Unauthorized and Malicious Access and Actions". [What system managers may do without further authorization is described above in the rule "System Managers".]

No person may use, for any purpose whatsoever, any information in another person's files (including e-mail) that they have seen incidental to any legitimate or illegitimate activity without either a reasonable belief that the file was meant to be accessed by others or the explicit permission of the person to which the file is assigned. It may be implicitly presumed that files shared by an experimental collaboration or other workgroup have the permission of all members of the group to be used by other members for purposes related to the mission of the group. An employee's (or user's) files, with the exception of files on backup media, that remain after the employee termination process is completed (expiration of user's validation) may be transferred as directed by the employee's supervisor (user's spokesperson) without further permission.

The following paragraph describes a standing exemption from these restrictions for specified computer security personal. Other exceptions to these restrictions require the written approval of the Director, Deputy Director, or an Associate Director (with copies of these approvals maintained in the Office of the CSExec). Such exceptions will normally be made only in serious disciplinary or legal situations.

Members of the Fermilab Computer Incident Response Team (FCIRT) as well as the FCSC and Deputy FCSCs may monitor computing activities and access and inspect any files or email in the course of carrying out their computer security preventive and response functions. Information learned in this way which is pertinent to computer security may be shared discreetly with others including supervisors and local system managers. Information not pertinent to computer security will be kept in confidence. Evidence of egregious behavior (serious violations of Fermilab rules,

[8] At this time, "large experiments" include CDF and D0. In the future, other active major experiments, such as CMS, MINOS, etc., will be added to this list.

criminal activity, etc.) that is uncovered incidental to such computer security related inspections will be reported to the CSExec for possible action through the Laboratory's normal channels.

Software Intellectual Property (Licenses)

Employees and users of Fermilab computing are reminded that it is Fermilab policy to respect the intellectual property rights of others. This applies when computers are involved just as it does when computers are not involved. Fermilab expects reasonable care be taken to follow license provisions.

2. Publishing and Accessing Information on Electronic Networks

The technology of the international computer network (Internet) and the evolving applications and standards that support it (especially the World Wide Web) provide unprecedented power to access and publish information almost instantaneously. Its impact on the collaborative field of high energy physics is particularly profound. It is an ideal tool for communication in the field. Fermilab strongly encourages its use.

This new capability comes with new challenges and individual responsibilities since this technology invites a much more immediate and wide dissemination of information. Despite the new power of this technology, the fundamental policy of Fermilab, and of its parent agency, about information and the use of our computers and networks remains unchanging and simple:

- Fermilab's single mission is science and the laboratory will maintain an open scientific environment where the free exchange of ideas is encouraged and protected.

- The use of government property is for the government's purposes.

There is no real conflict between these two principles since Fermilab's mission is for the government's purposes. The problem is in the interpretation of which ideas and what information are in the interests of Fermilab's science and open environment. Fermilab's policy is to take the broadest possible interpretation. There is a large gray area, and, to protect the continuing free exchange of ideas, it is the responsibility of every Fermilab employee and user to use common sense and good judgement.

Some material is not in the gray area. Sexually related material is clearly inappropriate, and when found either on Fermilab computers or posted externally from a Fermilab network address, Fermilab will initiate disciplinary action, including suspension without pay for employees, or suspension of site and computer access privileges, for users. In some cases, certainly those involving the felonious possession of pornography involving children, the government will take criminal action. Other legally prohibited material could also bring severe disciplinary or criminal sanctions.

Many people access the network and its postings. Most of them are from outside the scientific culture, and they may not understand how a particular posting may be related to the government's business. Therefore, it is Fermilab's policy that material that is published or posted with external visibility must be predominately clearly related to Fermilab's scientific mission.

The ease of use of this technology breaks down traditional mechanical barriers to publication prior to review. The disappearance of these barriers does not permit bypassing established rules and procedures regarding publication. For the purposes of these rules and procedures, electronically posted information with visibility external to the Fermilab community is to be understood as a public document.

The many crosslinks possible (on The Web, for example), and their ephemeral nature, means that pointers (links) to external addresses can quickly become a source of embarrassment. Employees and users should use common sense in displaying links on pages with Fermilab addresses; a link

should only point to material that is predominately appropriate reference material -- and likely to stay that way.

Scope

The policies described in this document apply to material posted on or retrieved from network addresses or domains owned or managed by Fermilab (e.g., fnal.gov, fnal.org, hep.net, auger.org, sdss.org, vlhc.org, scitech.mus.il.us, etc.). The applicability is not determined by who owns the computer or whether the data is physically stored on site or offsite or by the method of connection to the network. Fermilab employees and registered users are responsible for their own actions under this policy, as well as for the actions of any person who they permit to access a Fermilab computer system to post or retrieve material.

Public Availability versus Restricted Access

As an institution whose primary mission is to produce and disseminate new scientific information, Fermilab encourages the unrestricted publication on the Internet of as much of its internal material as possible. However, there may be reasons to restrict access to specific material, for example, its proprietary nature, security considerations, possibility of misinterpretations that could cause embarrassment, scientific work in progress, etc.

Division/Section Heads and Spokespersons are responsible for determining the classes of material within their organizations that should be restricted for access only by the Fermilab community or by defined subsets of the Fermilab community. The Computing Division World Wide Web Group will provide detailed instructions on implementing various options to restrict access for popular web servers. Options include restriction by password or IP address.

Material Intended for the Lay or Scientific Public

The Head of the Directorate's Office of Public Affairs has the responsibility for maintaining a home page and auxiliary pages presenting Fermilab to the public. Other laboratory entities may also provide such public information. In each such case where material is intended for the broad lay or scientific public, there must be an individual, approved in writing by the Head of Public Affairs, a Division/Section Head, or a Scientific Spokesperson, and identified on the electronic page, with responsibility for the material.

Externally Accessible Material Not Intended for the Lay or Scientific Public

Approvals are not required for material that is externally accessible but not intended primarily for the public. However, such material is subject to this policy and Division/Section or Spokesperson policy on content that may be posted for external access.

Professional (Personal) Home Pages

Individuals may publish professional (personal) home pages subject to this policy and to the policy of their Division/Section Head or Spokesperson as to content which may be posted for external access.

Semi-Official and Public Web Pages

Semi-official and pages intended for the public web pages require special considerations. The following would be examples of pages with unrestricted external access that are considered to be "semi-official":

- the page indicates that it is sponsored by a division, section, department, experiment, or other laboratory sanctioned organization
- it provides general institutional and/or technical information to laboratory staff, visitors, or the public
- it makes available a general laboratory service that is part of the mission of a Division, Section, or Department.

We do not include in this category pages that are working documents, such as computer codes, technical papers, professional home pages, etc.

The public and government agencies subject to particular scrutiny semi-official pages and pages intended for the public that have a .gov address. Division, section, and experiment management should pay particular attention that the content of these pages be generally seen as appropriate and inoffensive.

Semi-official pages and pages intended for the public are required by the Department of Energy to carry a legal notice. This notice should be implemented by including a link on each such page to http://www.fnal.gov/pub/disclaim.html

Web Crawler Controls

Web crawlers such as Yahoo, Alta Vista, or FirstGov, may index all pages with unrestricted external access. Even accidentally inappropriate wording (in computer codes or minutes, for example) are likely to be indexed and provide fodder for the salacious-minded.

Relatively simple methods exist for directing cooperating web crawlers, or "robots", not to index certain web sites or follow links found there. Consult the guidance document at http://www.fnal.gov/cd/webgroup/webhelp/access.html.

A preference not to index should only be used on working documents. Because the public or off site members of the Fermilab community may have a need to search in a public web crawler for information in Semi-Official pages, such pages should not be marked "do not index".

Cookies

The DOE strongly discourages the use of cookies. They should not be used on web pages intended for the general public. If you have a very strong technical or administrative reason to use cookies on a page intended for internal use, check with the computer security organization for guidance. There are no restrictions on the use of cookies on pages that are not visible from off-site.

Collecting Information from Children

The Children's Online Privacy Protection Act, effective April 21, 2000, applies to the online collection of personal information from children under 13. It is Fermilab policy not to collect personal information from children under 13.

Privacy and Information Collected from the Public

It is Fermilab's policy that any information collected electronically from the public not be used for any external or commercial purposes, whether this information was collected intentionally or not. You should deal with any such collected information in conformance with the Fermilab Privacy Notice published at www.fnal.gov/pub/disclaim.html.

3. Use of Computers in Systems that Protect People, Property, or the Environment

Since the earliest days at Fermilab, it has been our policy to avoid reliance on a computer as an essential element of any system that is necessary to protect people from serious harm, to protect the environment from significant impact, or to protect property the loss of which would have a serious impact on our mission.

The use of computers for monitoring, data logging, and reporting is encouraged, however computers used for these purposes must not be essential for protection.

Any variation from this policy on protection systems must have the written concurrence of the Fermilab Senior Computer Security Executive (CSExec) and the Associate Director for Operations Support (ADOS).

A committee appointed by the CSExec and ADOS will consider variances from this policy for systems designed in accord with ANSI/ISA S84.01-1996 at levels 3 or 4 after a detailed review of the plan. In particular, the system must be isolated from the Laboratory network and the Internet at all times, and its program must never have been exposed to these networks and must be traceable to program source code that has been reviewed by the above committee.

4. Special Policies and Rules for the Strong Authentication Realm

Most of this section is technical and addressed at system managers of systems in the Fermilab Kerberos (or "strengthened") realm[9].

The motivation for Fermilab's move to a strong authentication realm includes the following goals:

- elimination of clear text passwords on the network,
- elimination of crackable password files on systems,
- a single password and/or cryptocard for each user,
- the expectation of the United States Government that Fermilab management will exercise positive control of those who use the government's resources, including Department of Energy owned computers and the network, at the Fermilab site,
- maintaining the free and open access to Fermilab's scientific activities and information by the international high energy physics community.

In order to meet these goals, the present plan calls for the whole Fermilab site to be in the strengthened realm by the end of 2001.

Consistent with the motivations cited above, we do not require Kerberos authentication for uses which involve only reading information (via the Web or ftp, for example), or only entering information into a Web or data base form[10], even if a password is required by the local organization or collaboration. All other uses of computers or the network within a strengthened realm must be preceded by Kerberos authentication that will verify that the user is either a Fermilab employee or an onsite or offsite user who has registered with the Users' Office. This does not mean that all computers or applications within the strengthened realm are required to use Kerberos authentication. It does mean that before using a computer that does not do Kerberos authentication an individual must pass through either a computer that does a Kerberos authentication or through a computer to which physical access is restricted to individuals carrying a valid Fermilab ID card .

The following policies are in force for protection of user authentication in the Kerberos (or "strengthened") realms. Distinctions are made between systems on-site and those at visitors' home institutions. For all on-site "strengthened" systems, all network access which provides access comparable to system login, shell execution or file transfers (other than anonymous) must only be authenticated by Kerberos credentials presented with the connection setup, or by a single-use authentication mechanism (such as a Cryptocard) tied to the Kerberos infrastructure. Off-site

---

[9] On-site or off-site computers in the "Strengthened Realm" are those on which users may be authenticated for access to systems on the Fermilab network by a Fermilab Kerberos Key Server. Also in the "Strengthened Realm" are computers to which user access is controlled by restricting connections to pass through a computer that provides the Kerberos authentication for access.

[10] It is required that a user be Kerberos authenticated within the Strengthened Realm prior to that user entering information into a form on a computer in the Strengthened Realm for any purpose where incorrect or inappropriate entry could cause damage to Fermilab resources or disruption to Fermilab activities. This includes, but is not limited to, entry of data to be used to set control values for equipment (including accelerator, beam, detector, building, etc.) or to be used for computer system management or configuration purposes.

systems (and any on-site systems in the "pilot" realm, until that realm is finally phased out[11]) may optionally accept encrypted connections using non-Kerberos authentication mechanisms.

In any case, offsite systems joining a Fermilab Kerberos realm must be covered by a written policy stating that insecure access mechanisms (including cleartext reusable passwords and "traditional r-command" methods) will not be permitted, and must adhere to said policy.[12]

On- and off-site systems in our Kerberos realm will be probed over the network to try to verify compliance with these conditions. Hosts found to be noncompliant may be barred from obtaining Kerberos tickets from our realm. If the noncompliance is deliberate or extremely careless it may be deemed to constitute blatant disregard for computer security.

Publication Date: August 20, 1998
Revision: September 4, 2001

[11] The "pilot" realm will be considered phased out on June 30, 2001. This is four months after the official scheduled start of Run 2. If the run is delayed significantly, the final phase out date may be extended. After this date, all on-site strengthened realm systems will be restricted to Kerberos authentication only. The Computing Division will provide assistance wherever possible to system managers to set up Kerberos authentication. It is recommended that managers of non-Fermilab owned systems in the strengthened realm accomplish the transition to Kerberos authentication as far in advance of June 30 as possible.

[12] It is expected that the written policy will list the systems covered by the policy and what combinations of access (e.g., ssh, telnet, ipsec) and authentication (RSA keys, passwords, one-time passwords, etc) are allowed on those systems. It must also give a means of contacting the system administrator(s). If a written policy against allowing insecure access to such systems meeting these requirements already exists, it may be used. If none exists, one can be drawn up for the purpose.